REMARKS

Claims 1-30 are pending and are unamended. Withdrawal of all objections and rejections are respectfully requested for at least the reasons set forth below.

Examiner Interview

Applicants wish to thank Examiner Leroux for extending the courtesy of a telephone interview in respect to this application on August 5, 2004 with Applicant as represented by joint inventor Adam Schran and Applicants' undersigned representative. During the interview, a previously faxed Draft Response was discussed. No agreement was reached regarding allowability of the pending claims, but the Examiner agreed to review the arguments that highlight the significant differences between the claimed invention and the applied references upon formal submission of a response. One key point discussed during the interview is that exemplary claim 1 is directed to a specific process to assist a user in screening cookie files, not to the very concept of the cookie itself as described in Montulli. The Examiner also requested that Applicants provide a concise explanation of how the claimed invention differs from the applied references. In addition to the differences discussed below, one important distinction is provided in the following paragraph.

All of the pending claims require a "list of cookie file sources." A "cookie file source" is defined on page 5, lines 28-29 of the specification as being "a website, an e-business or any other entity that sends cookie files." A list of cookie files sources therefore is either a list of websites, a list of e-businesses, or a list of entities that send cookie files. A list of cookie files sources is completely different than a list of cookies (alternatively, referred to as "cookie files"), such as the list of cookies stored in the well-known cookies.txt file of a browser program. In one preferred embodiment of the present invention, the claimed list of cookie files sources may be used to manage the list of cookies stored in the cookies.txt file of a browser program. Montulli and Wagner both disclose the use of a conventional list of cookies stored in a file of a browser program. However, neither Montulli nor Wagner disclose or suggest requesting, receiving, downloading, or using a list of cookie file sources as set forth in step (a) of claims 1, 12, 16 and

27, and step (c) of claims 7 and 22, or any of the remaining steps in these claims that use the list of cookie file sources.

Prior Art Rejections

Claims 1, 3-5, 16 and 18-20[1] were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,826,242 (Montulli). Claims 2, 6-15, 17 and 21-30[2] were rejected 35 U.S.C. § 103(a) as being unpatentable over Montulli in view of U.S. Patent No. 6,085,224 (Wagner).

1. Claims 1 and 16 are patentable over Montulli ('242)

a. Remarks repeated from first Office Action

Claim 1 is directed to a method of screening cookies in a client machine. A server receives a request from a subscriber to send a list of cookie file sources to the client machine. The list is downloaded from the server to the client machine. The downloaded list is then used to detect cookie files received at the client machine from sources on the downloaded list.

In one embodiment of the claim 1 invention, the list may include web sites (cookie file sources) which are known to send cookies that when stored on a user's computer compromise a computer user's privacy. For example, some web sites send out cookies that track a user's web site navigation and report the results back to a designated web site, all without knowledge to the user. See, for example, the discussion of how DoubleClick cookies are used on page 13 of Appendix A[3] filed in the Response to the first Office Action.

It is virtually impossible for an individual computer user to keep track of all of the web sites that send out undesirable cookies. The method in claim 1 allows a monitoring entity (e.g., a service provider) to keep track of such web sites and send a list of such web sites to a client machine upon request. During subsequent navigation by a user at the client machine, the list can be used to detect cookie files when a web site on the list is encountered by the client machine.

---

[1] The Examiner's reference to claims "18 and 19" appears to be an error and should have read "18-20."

[2] The Examiner's reference to claims "20-30" appears to be an error and should have read "21-30."

[3] Shah, R.C. et al. "Governance Characteristics of "Code": The Role of Transparency, Defaults and Standards," 2002 Telecommunications Policy Research Conference, September 28-30, 2002, Alexandria Virginia, article posted on web site: http://intel.si.umich.edu/tprc/papers/2002/90/TransparentDefaultStandards.pdf, printout date: October 23, 2003, 30 pages (Appendix A includes pages 1 and 10-14 only).

Upon detection, the cookies files can be removed from the client machine and/or prevented from being stored, as recited in dependent claims 5 and 6. (Independent claim 1 is more broadly directed to using the list to detect cookie files.)

Montulli ('242), hereafter, "Montulli," is a well-known patent that is touted as describing the original concept of a cookie. See page 11 of Appendix A filed in the Response to the first Office Action, especially footnote 20. (U.S. Patent No. 5,774,670 is the parent patent of Montulli '242.) The portions of Montulli referenced by the Examiner in the outstanding Office Action merely describe the purpose of a cookie, how cookies are sent, and what they do on a client machine. Montulli thus describes sending and using cookie files. Nowhere does Montulli describe creating lists of cookie file sources (claim 1 step (a)), downloading cookie file lists (claim 1, step (b)), or using a downloaded list to detect cookie files (claim 1, step (c)). Claim 1 is directed to a specific process to assist a user in screening cookies files, not to the very concept of a cookie itself as described in Montulli.

To anticipate a method claim, a reference must disclose each and every step in the claim. Here, Montulli fails to disclose any of the steps in claim 1. In sum, Montulli has nothing whatsoever to do with the claimed invention and thus the rejection of claim 1 over Montulli should be withdrawn.

Claim 16 is similar to claim 1 and is thus patentable over Montulli for the same reasons as discussed above with respect to claim 1.

b. New remarks

Claims 1 and 16 are directed to a specific process to assist a user in screening cookies files, not to the very concept of a cookie itself as described in Montulli.

In the present Office Action, the Examiner highlights column 8, lines 1-4; and column 9, lines 18-36 and 53-63 of Montulli for allegedly disclosing downloading a list of cookie file sources and using the downloaded list to detect cookie files received at the client machine. In fact, these portions of Montulli do not disclose downloading cookie file sources, but instead disclose downloading cookie file lists, maintaining a list of the downloaded cookie files at a client machine and using cookie files in the maintained list at the appropriate time (e.g., when a web page/web site associated with a cookie file is requested by the client machine). One or more

cookies are typically downloaded to a client machine as hidden data file(s) piggybacked onto a web page requested by the client machine. When the client machine receives the data file(s), it directs the client machine to store the cookie(s). When subsequent requests are made by the client machine for a web page/web site associated with the cookie(s), the cookie data is sent to the requested web page/web site and causes certain actions to be taken by the web page/web site, as described on column 9, lines 53-64 of Montulli. For example, a cookie may cause a web site to return a web page customized in some manner (e.g., language, content) based on cookie data. There are endless uses for cookies but one common use of cookies is to customize a user session experience based on the content of the cookie. Browsers have designated locations for storing cookie files and browsers provide tools for allowing a user to view and edit the cookie files on the client machine. A full discussion of this cookie handling process can also be found in the Background of the Invention section of Wagner.

Montulli and the present invention thus have one feature in common which is that both download and make use of a list of cookie files stored on a client machine. Montulli's list of cookie files is built as a client machine accesses additional web pages/web sites, thereby causing new cookies to be added to the cookie files on the client machine for each accessed web page/web site that employs cookies. The "set-cookie command" described on column 9, lines 19-20 of Montulli directs the client machine to store the cookie associated with the requested web page/web site. In Montulli's scheme, no process exists to ask for a download of a list of cookie file sources, nor is any scheme contemplated in Montulli wherein a plurality of cookie file sources are downloaded to the client machine. All that Montulli describes is the conventional process for receiving, storing and subsequently using any cookies that reach the client machine after being piggybacked onto a web page/web site sent to a client machine. The cookie file list used in Montulli is a separate object from a cookie file source list. Montulli discloses only the cookie file list, whereas the present invention discloses and uses both. That is, the present invention makes use of both a cookie file source list as well as a cookie file list. More specifically, the cookie file source list is used to control and manage the contents of the cookie file list.

The present invention is thus entirely compatible with Montulli and can be used as an adjunct to the cookie handling process described in Montulli. That is, the cookie file source list

of the present invention can be used to control and manage the cookie file list in Montulli. However, nowhere does Montulli disclose or suggest any of the steps in claims 1 or 16.

2. Claims 7 and 12 are patentable over Montulli in view of Wagner

Claim 7 is directed to a method of creating a composite list of cookie file sources in a client machine. A first exception list is created that includes the identity of sources that are permitted to store cookie files in the client machine. A second exception list is created that includes the identity of sources that are not permitted to store cookie files in the client machine. A client machine receives a master list of cookie file sources from a service provider. The master list is then modified in accordance with the first and second exception lists. The composite list is the modified master list.

Claim 12 is also directed to a method of creating a composite list of cookie file sources in a client machine. A master list of cookie files sources is received at the client machine from a service provider. Cookie file sources on the master list that correspond to one or more trusted cookie file sources listed in the client machine are deleted. Cookie file sources that correspond to one or more untrusted cookie file sources listed in the client machine are added to the master list. The composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

Wagner discloses a software program that intercept and scans "downloadable technologies" such as Java, ActiveX, cookies, and JavaScript before they enter a user's machine. As described above and as extensively described in the Background section of Wagner, cookies are sent to a user's machine as hidden data files attached to requested web pages. Wagner's software has been commercialized as a product called "X-Ray Vision." See the article descriptions of the software in Appendix B attached hereto. The following excerpts from the articles explain what the software does:

> In response to this phenomenon, a product has been designed to intercept and scan these "downloadable" technologies - Java, ActiveX, cookies, JavaScript - before they enter a user's machine. X-Ray Vision, created by the Atlanta-based Intracept Inc., prevents any transmission or retrieval of data between a Web site and a computer.

> "We want to let you see who's watching you while surfing on the Net," said Richard Wagner, president of Intracept. "We'll disable them (downloadables), and if the user wants to reload with them turned on, it's only a few mouse-clicks away."
>
> To prevent Web sites from placing or collecting information from a machine's hard drive, X-Ray Vision can be set up to block any or all downloadable technologies; it can also be configured to alert the user as to which downloadables are present, blocked, and allowed. And unlike other security products, which download first and ask questions later, Wagner said, X-Ray will prevent a Web page from launching them in the first place.
>
> X-Ray Vision keeps your system secure and protects your privacy while you surf the Web. X-Ray Vision intercepts and scans all data before it enters your browser or leaves your PC through the Internet. With its customizable security levels, it prevents a Web site from obtaining data from your PC, launching programs on your PC, or accessing your PC. It also provides you with information on the administrator of any Web site you visit.
>
> The program identifies and blocks the widest range of downloadable technologies, including ActiveX applets, Java applets, JavaScript, Visual Basic Script, Cookies, Plug-ins and Server push and pull commands. You can individually customize the level of security for each Web site you frequently visit. Cookies can be deleted at any time (without annoying cookie alerts) and there is an option to automatically clean your cache each time you start your browser.

Neither Wagner's patent nor the description of Wagner's software discloses or suggests creating exception lists or master lists of cookie file sources, nor modifying (e.g., adding or deleting) entries in a master list of cookie file sources received from a service provider. Instead, Wagner processes cookies files on an individual basis based on prescribed rules set up by the user's computer, particularly the rules prescribed in Wagner's "action map." Wagner thus does not disclose or suggest any of the steps of claims 7 or 12.

With respect to claim 7, the Examiner asserts that column 2, lines 28-37 of Montulli discloses a service provider master list of cookie files sources, and that column 8, lines 1-4 and column 9, lines 18-36 of Montulli discloses modifying the master list in accordance with first and second exception lists. This is incorrect. The above-highlighted passages of Montulli describe the conventional use of cookies wherein they are received from a remote server, stored

in a client's computer, and then accessed and sent to the remote server the next time that the user requests a document from the same server. As described above, a list of cookie files are stored in the user's computer, but this list is not a list of cookie file sources which is a separate object in the present invention than the list of cookie files. (Both exist in the present invention.) There is no downloading of a master list of cookie file sources to create this list. Furthermore, the cookie list stored in the client machine is not modified as a result of exception lists. Modifications are made over time based on other factors known to those skilled in the art, such as an expiration of a cookie, reaching capacity limits (e.g., in the example described on column 9, lines 18-35 of Montulli, the cookie list has preprogrammed limits, such as 300 total cookies), overwriting of an existing cookie with a new cookie from the same server or domain, or a user or program opening the cookie file and selecting some or all of the cookies for deletion.

The Examiner also asserts that column 9, lines 29-65 of Wagner discloses exception lists. This is also incorrect. This portion of Wagner describes the action map which defines how incoming and outgoing cookies are to be treated when a request is made to or from a specific server. One function of the action map is to examine HTTP headers and to make decisions regarding treatment of cookies associated with the server site based on the header data. The action map is a series of rules, and has no list of cookie file sources. No exception list is used in this process.

With respect to claim 12, the Examiner highlights similar portions of Montulli and Wagner for allegedly showing the three steps in claim 12. None of these claimed steps exist in either of these references for the same reasons as discussed above with respect to claim 7.

The combination of Montulli and Wagner would allow for enhanced user control of cookies. However, the combination of these references fail to disclose or suggest any of the steps in claims 7 or 12.

To render obvious a method claim or an article of manufacture claim, an applied reference or combination of applied references must disclose each and every step in the claims. Here, Montulli and Wagner fail to disclose any of the steps in claims 7 or 12. In sum, neither of these references have anything to do with the claimed invention and thus the rejection of claims 7 and 12 over these references should be withdrawn.

Claims 22 and 27 are similar in scope to claims 7 and 12, respectively,, and are thus patentable over the applied combination for the same reasons as discussed above with respect to claims 7 and 12.

3. Patentability of Dependent Claims 2-6, 8-11, 13-15, 17-21, 23-26 and 28-30

The dependent claims are believed to be allowable because they depend upon respective allowable independent claims, and because they recite additional patentable steps.

With respect to dependent claims 2, 6, 17 and 21, Wagner does not make up for any of the highlighted deficiencies in Montulli.

Conclusion

Insofar as the Examiner's rejections were fully addressed, the instant application is in condition for allowance. Issuance of a Notice of Allowability of all pending claims is therefore earnestly solicited.

Respectfully submitted,

ADAM R. SCHRAN et al.

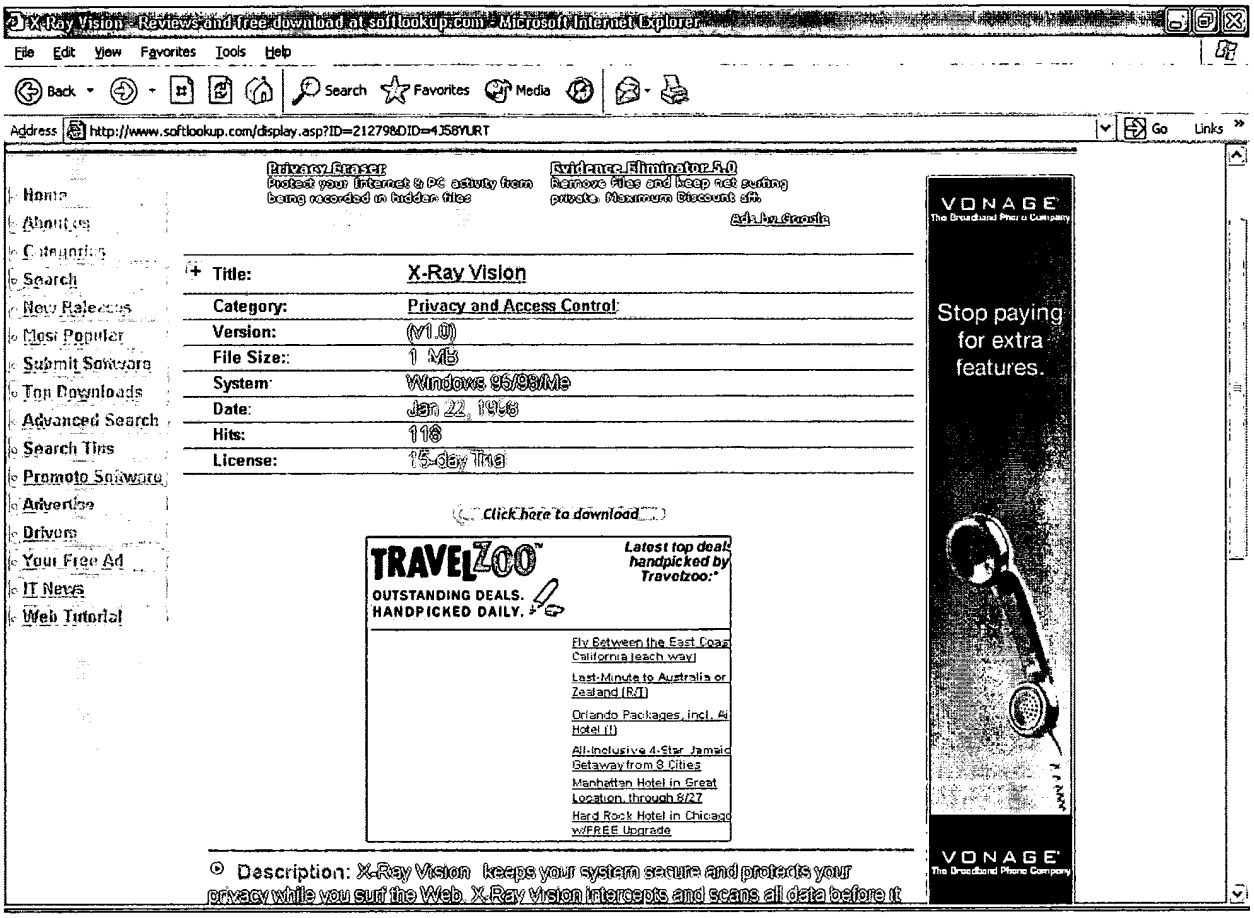
August 17, 2004 By: Clark Jablon
(Date)

CLARK A. JABLON
Registration No. 35,039
AKIN GUMP STRAUSS HAUER & FELD LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1200
Direct Dial: 215-965-1293
Facsimile: 215-965-1210
E-Mail: cjablon@akingump.com

Enclosure (Appendix B)

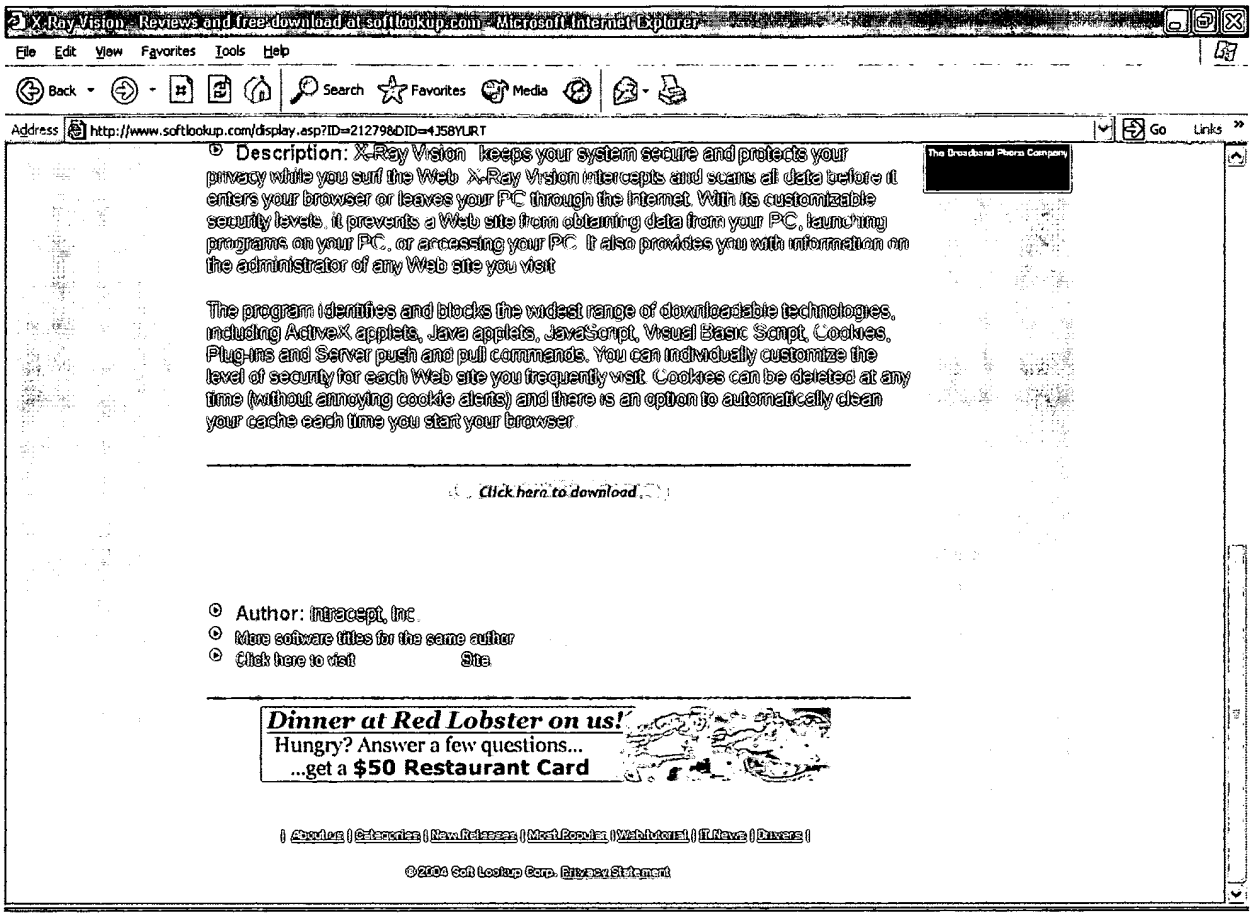
APPENDIX A

See Appendix A attached to Response to Office Action mailed October 24, 2003 (filed February 4, 2004)



APPENDIX B

(Application No. 09/820,054
Reply to Office Action of April 21, 2004)



Description: X-Ray Vision keeps your system secure and protects your privacy while you surf the Web. X-Ray Vision intercepts and scans all data before it enters your browser or leaves your PC through the Internet. With its customizable security levels, it prevents a Web site from obtaining data from your PC, launching programs on your PC, or accessing your PC. It also provides you with information on the administrator of any Web site you visit.

The program identifies and blocks the widest range of downloadable technologies, including ActiveX applets, Java applets, JavaScript, Visual Basic Script, Cookies, Plug-ins and Server push and pull commands. You can individually customize the level of security for each Web site you frequently visit. Cookies can be deleted at any time (without annoying cookie alerts) and there is an option to automatically clean your cache each time you start your browser.

WIRED NEWS

Home | Technology | Culture | Business | Politics | Wired Mag | Animation

Text Size: A A A A

Shutting the Door on Cookies and Applets

Christopher Jones

Story location: http://www.wired.com/news/technology/0,1282,7975,00.html

03:08 PM Oct. 24, 1997 PT

The Web, aside from its impact on the computer industry, has also brought on a marketing bonanza. As unsuspecting users bound about the Web, cookies, applets, and other seemingly innocuous programs are tracking their every move, recording data that will prime the pumps of many new, Web-based marketing and advertising campaigns.

In response to this phenomenon, a product has been designed to intercept and scan these "downloadable" technologies - Java, ActiveX, cookies, JavaScript - before they enter a user's machine. X-Ray Vision, created by the Atlanta-based Intracept Inc., prevents any transmission or retrieval of data between a Web site and a computer.

"We want to let you see who's watching you while surfing on the Net," said Richard Wagner, president of Intracept. "We'll disable them (downloadables), and if the user wants to reload with them turned on, it's only a few mouse-clicks away."

To prevent Web sites from placing or collecting information from a machine's hard drive, X-Ray Vision can be set up to block any or all downloadable technologies; it can also be configured to alert the user as to which downloadables are present, blocked, and allowed. And unlike other security products, which download first and ask questions later, Wagner said, X-Ray will prevent a Web page from launching them in the first place.

"Information being stored on a user's computer without them knowing it is not necessarily harmful or malicious, but when you look at the entire scope of what can happen, there are a number of different hazards a user can run into," said Wagner, adding that 80 percent of the top 100 visited Web sites now employ downloadable programs.

Although the occurrence of malicious applets or ActiveX controls is, as yet, uncommon, the emergence of more executable programs on the Web has prompted existing security vendors to develop technologies that block and

monitor these applications as well. Finjan Software is one company that has built a business around blocking Java applets and ActiveX controls, and major companies like Cisco, CheckPoint, and DEC plan to incorporate its technology into other products, primarily firewalls.

Related Wired Links:

Next Netscape Will Chew Cookies on Command
22.Feb.97

Junkbuster Strips Banners, Cookies
22.Feb.97

Group Seeks to Put Lid on Pandora's Cookie Jar
7.Apr.97

-5 of 5-